

# Claims

- [c1] A method for facilitating biometric security in a smart-card transaction system comprising:
  - detecting a proffered biometric at a sensor communicating with said system to obtain a proffered biometric sample;
  - verifying the proffered biometric sample; and
  - authorizing a transaction upon verification of the proffered biometric sample.
- [c2] The method of claim 1, wherein said step of detecting further includes detecting a proffered biometric at a sensor configured to communicate with said system via at least one of a smartcard, reader, and network.
- [c3] The method of claim 1, wherein said step of detecting includes at least one of: detecting, storing, and processing a proffered biometric sample.
- [c4] The method of claim 1, wherein said step of detecting further includes receiving a finite number of proffered biometric samples during a transaction.
- [c5] The method of claim 1, wherein said step of detecting includes logging each proffered biometric sample.

- [c6] The method of claim 1, wherein said step of detecting further includes at least one of detecting, processing and storing at least one second proffered biometric sample.
- [c7] The method of claim 1, wherein said step of verifying includes comparing a proffered biometric sample with a stored biometric sample.
- [c8] The method of claim 7, wherein comparing a proffered biometric sample with a stored biometric sample includes comparing a proffered biometric sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.
- [c9] The method of claim 1, wherein said step of verifying includes verifying a proffered biometric sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.
- [c10] The method of claim 1, wherein said step of verifying includes verifying a proffered biometric scan sample using one of a local CPU and a third-party security vendor.